Workshop Schedule
Wednesday

- 8am - 9am: Walk-through of a sample PP
- 9am - 10am: Threat Analysis Review
- 10am - noon: Mini-Threat Analysis Exercise
- 12pm - 1pm: Lunch
- 1pm - 2pm: Security Objectives Review
- 2pm - 4pm: Security Objective Development Exercise

Advanced Exercises

Threat Analysis

- Threat Agent

- The Attack

- Assets

Types of Possible Threat Agents

- Disgruntled/Former Employees
- Industrial Competitors
- Hackers
- Incompetent Employees
- Criminal Elements
- Organized Crime
- Terrorists
- Foreign Intelligence
- Natural Disasters

Potential Motivations for an Attack

- Gain access to classified, sensitive, or proprietary data
- Track or monitor the target's operation
- Disrupt the target's operation
- Steal money, products, or services
- Obtain free use of resources
- Embarrass the target
- Accidental, i.e., no explicit motivation
- Mischief, boredom
- No chance of discovery/prosecution
- Revenge

Possible Attack: Intercept Attacks

- Monitoring of communications sent over public media (radio, satellite, microwave, public switched networks)
- Types of attack
  - traffic analysis/flooding the NW
  - monitoring of plain text communications
  - decrypting weakly encrypted communications
  - capturing ID numbers, names, and passwords
- Types of countermeasures
  - protected networks,protected passwords,public key
  - encryption of sensitive data
  - “onion” routing

Possible Attack: Network Based Attacks

- Attacks against NW backbone, insertion or modification of data in transit, electronic penetrations of boundary protection devices
- Types of attack
  - defeating login mechanisms
  - stealing protected sessions
  - masquerading
  - data manipulation
- Types of countermeasures
  - firewalls/guards, packet auth., digital signature
  - protected remote access
  - virus and intrusion detection tools
  - strong I&A
  - session encryption

Possible Attack: Insider Attacks

- Initiated by individuals that have authorized access
- Types of attack
  - compromise of data or access
  - modification of system protection measures
- Types of countermeasures
  - security awareness/training
  - audit and intrusion detection
  - specialized access control for critical data/products/services
  - strong identification and authentication capability
  - prosecution policies
  - roles/least privilege

Possible Attack: HW/SW Distribution Attacks

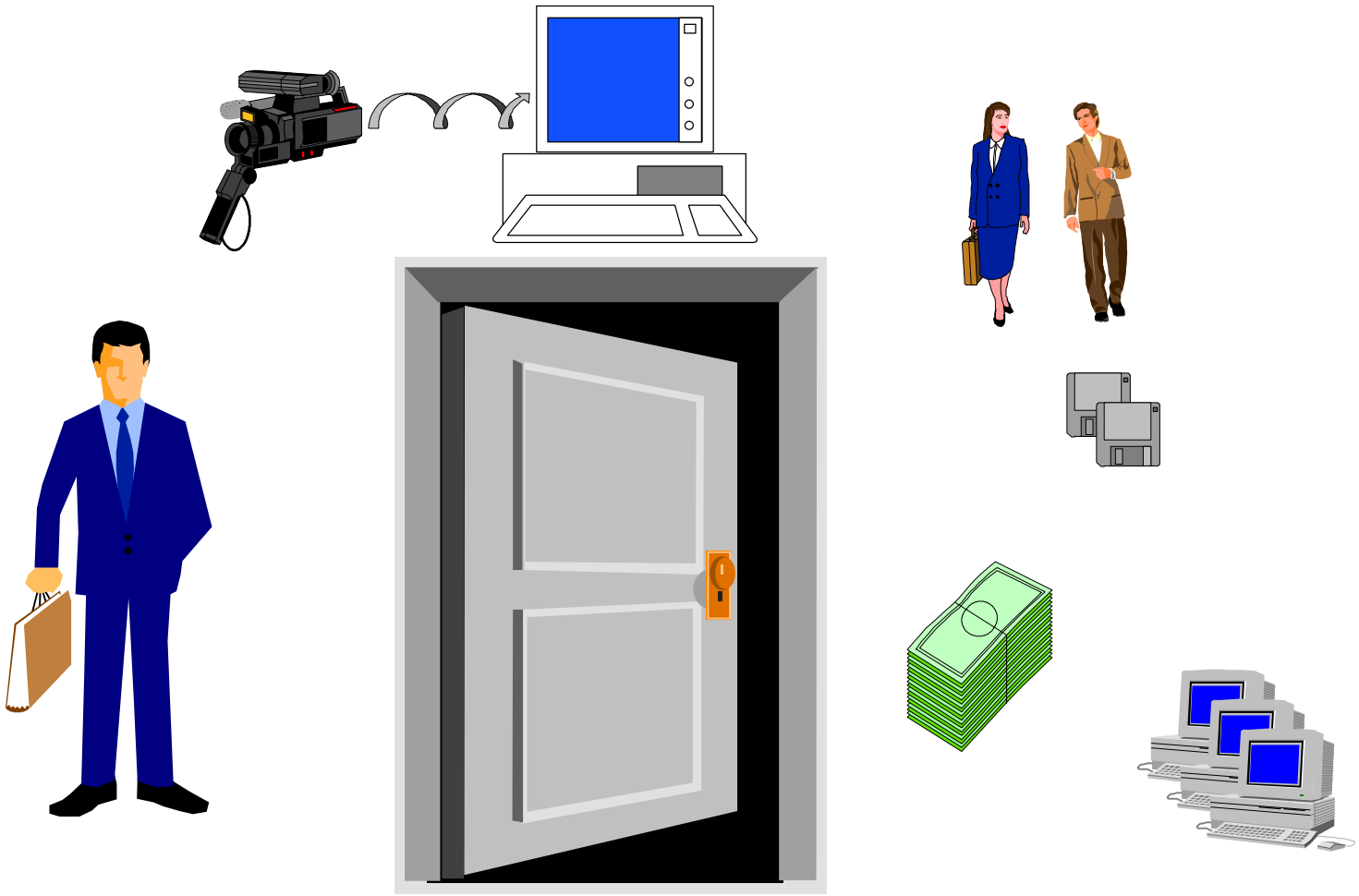
- Types of attack
  - modification of HW/SW at the factory
  - modification/substitution during distribution
- Types of countermeasures
  - strong in-process configuration control
  - controlled distribution
  - digitally signed or checksummed SW

Biometric Devices

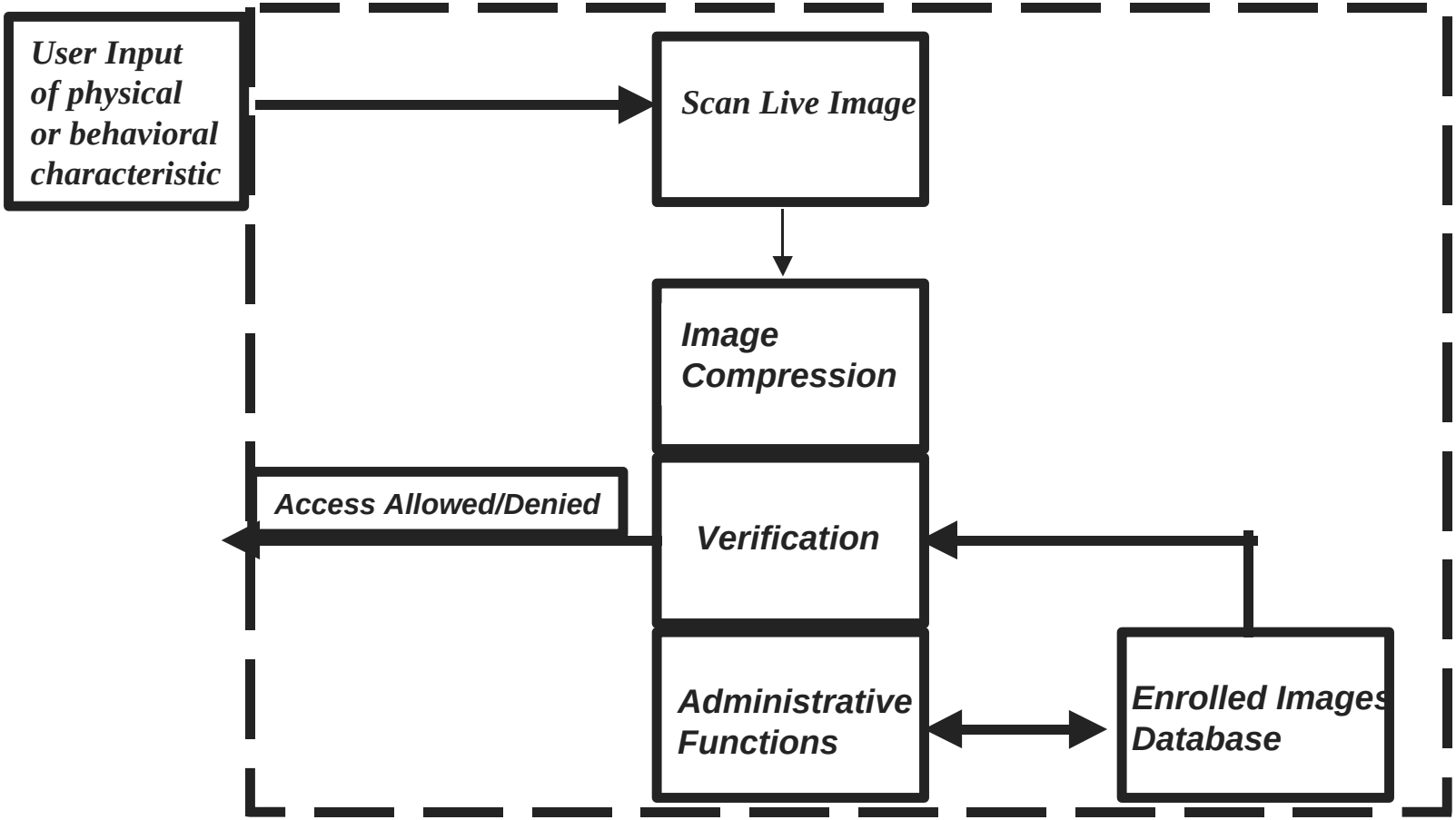
- A Biometric Device identifies an individual by examining a unique physical or behavioral characteristic

- Two types of Biometric Devices:
  - Who is this individual
  - Is the individual who they say they are

TOE Description



Biometric Device - High-Level Architectural Design



Mini Threat Analysis Exercise

- Brainstorming Technique will be used
- Choose a facilitator
- Use the white board to record ideas
- **ALL THREATS SHOULD BE CONSIDERED**

Limited Parameters for the Mini Threat Analysis

- The Biometric Device is a hand geometry scanner that controls access to safe deposit boxes
- The safe deposit boxes contain customer's valuables
- The threat agent could be an *authorized or unauthorized user*
- Assume the threat agent is unobserved

Brainstorming Technique

① Individual Work: 5-10 minutes for each person to attempt to come up with two possible attacks.

② Group Work: In round-robin fashion each person should describe one of their attacks which is recorded by the facilitator.

③ Brainstorming: Ideas that are generated as a result of the round-robin discussion should also be recorded. Record ALL ATTACKS no matter how bizarre!

③ Refine: Once all ideas are exhausted, revisit the list to eliminate any ideas that are not feasible given the environmental parameters.

Mini Threat Analysis Exercise

Biometric Device Protection Profile Overview

- The intent of this PP is to specify functional and assurance requirements applicable to commercially available Biometric Devices used to verify previously enrolled individuals for entry to a portal which protects assets.

- Assumption about the intended usage of the TOE:

  A.PORTAL Biometric Devices as discussed in this PP are intended to be used for authenticating individuals for entry to a portal. Once inside the portal, assets are not protected by the Biometric Device.

BDPP Overview (Con't)

- The BDPP includes requirements concerning:
  - connection between the scanning device (e.g.,camera, hand or iris scanner) and the HW/SW of the Biometric Device
  - connection between the HW/SW of the the Biometric Device and the portal

Threats to the Biometric Device

- Improperly adjusted FAR/FRR
- Impersonation of an authorized individual
- Attempts to exceed authority
- Taking advantage of the manual backup system
- Modification of data, configuration items, executables or H/W
- Flaws in the design
- Modification of the audit trail
- Failure to collect audit data
- Failure to review audit data
- Power loss
- Trap doors
- Electromagnetic flooding
- Physical attacks to connections

Secure Usage Assumptions

Identifies the significant assumptions made in the development of this PP; for example, security aspects of the environment in which the TOE will be used and how the TOE is to be used within this environment.

- Information about environment:
  - physical issues
  - connectivity issues
  - personnel issues
- Information about intended usage:
  - intended application
  - potential asset value
  - possible usage limitations

BDPP Secure Usage Assumptions

- **A.DEDICATED** The hardware that hosts the Biometric Device software is a dedicated machine.
- **A.SINGLE** The Biometric Device is intended to be used as a stand-alone device and is not part of a network.
- **A.PHYSICAL** The Biometric Device, and the HW and SW critical to security policy enforcement, is located within controlled access facilities which will prevent unauthorized modification by potentially hostile outsiders.
- **A.RELAY** The connection between the Biometric Device "reader" and the verification component, and the Biometric Device and the portal, is physically protected from unauthorized modification by potentially hostile outsiders.
- **A.NO_EVIL** Administrators and operators are assumed to be non-hostile and trusted to perform all their duties correctly. Developers of the Biometric Device are assumed to be trustworthy.

Organizational Security Policies

A set of rules, procedures, practices, and guidelines imposed by an organization upon its operations and to which the TOE must comply.

BDPP Organizational Security Policies

- Security Awareness Policy
- Manual Backup System Policy

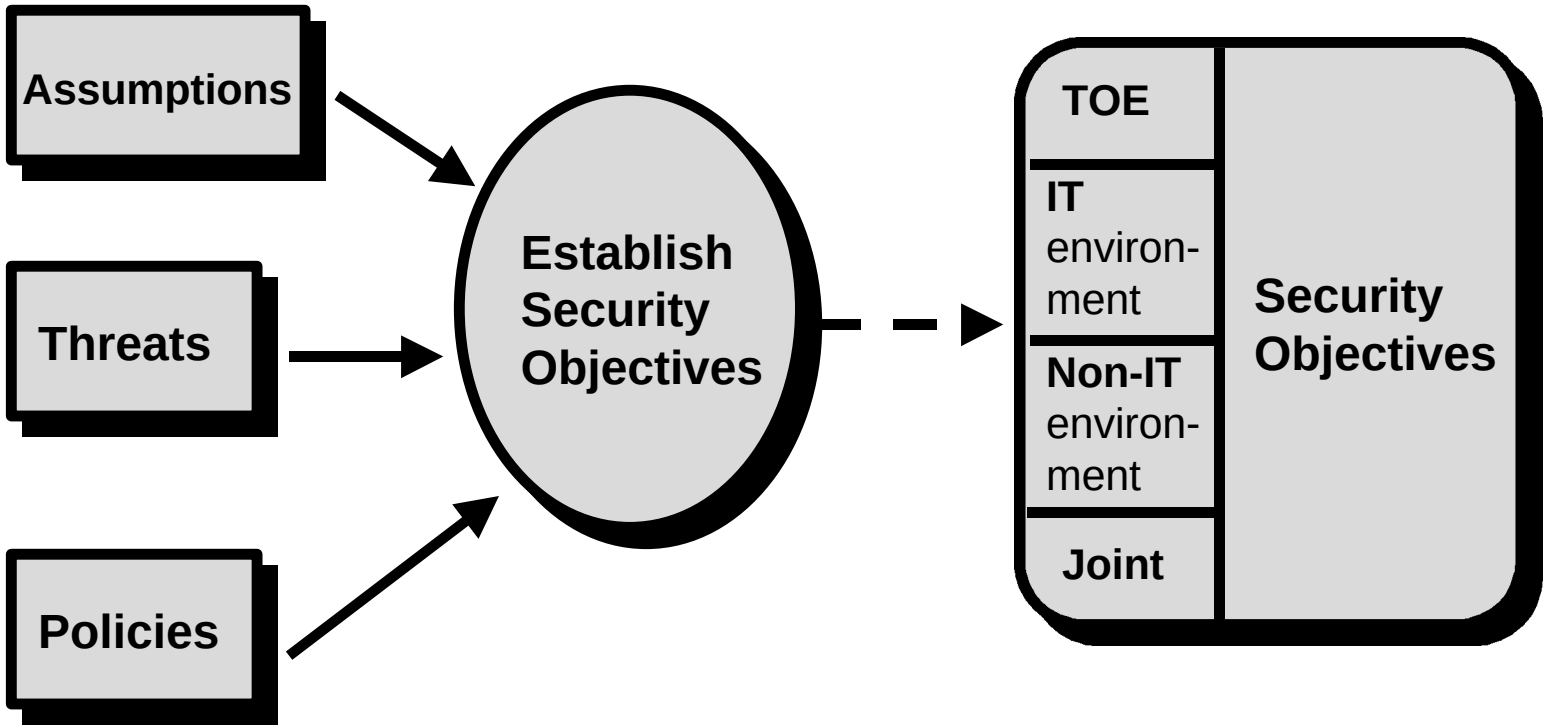
BDPP Training Policy

P.TRAIN All individuals who access any security-relevant device must receive training on the proper use of the device as well as security issues and vulnerabilities that arise from its improper use.

BDPP Manual Policy

P.MANUAL A manual means for opening the portal must be provided in the event of Biometric Device failure.

Security Objective Development



Security Objectives reflect the intent to counter identified threats and/or address any identified organizational security policies and assumptions.

Needs vs. Objectives

- A NEED is an urgent want or desire:

  A record of certain actions taken by users such that an administrator can determine when the action occurred, who did it, whether it succeeded or failed.

- An OBJECTIVE is the “end sought”

- OBJECTIVES are commitments aimed at *doing*, which also provide information on *how* a need will be met.

  – The TOE implementation must demonstrate that the industry required, minimum level of due diligence has been performed with respect to holding users of the TOE accountable for their actions.

CC Definition of Security Objective

- A statement of intent on how the derived requirements will
  - *counter* a given threat
  - *comply* with a given Organizational Security Policy

in light of the Secure Usage Assumptions

Properties of Useful Objectives

- Objectives define the strategy for implementing specific IT security needs in the intended environment
- Objectives must be operational, i.e., they must be capable of being translated into a set of requirements
- Objectives must be selective rather than encompass everything
- There must be multiple objectives in order to address the variety of needs
- Objectives are needed in all areas where policies and threats have been identified

Balancing Objectives

- Objectives must be balanced against attainability
- Objectives must be balanced against both immediate and future needs
- Objectives must be balanced against each other

How Do We Write Objectives?

- Consider the properties of good objectives
- Take advantage of security objectives in existing PPs and STs
- Use your
  - Knowledge of the TOE Technology
  - Experience with Security Issues
- Don’t forget to balance objectives

Identification of Security Objectives Exercise

- Use the assumptions, threats, and policies distributed
- A blank mapping table is provided in the student handbook

Identification of Security Objectives Exercise

Security Objective for the TOE: O.BYPASS

The TOE must prevent illicit individuals or errant software from bypassing TOE security policy enforcement.

Threats countered:

- T.IMPERSON
- T.BADUSER
- T.BADADM
- T.BADOPER

Security Objective for the TOE: O.ALLDEN

The TOE must allow entry to the portal to all authorized individuals and deny entry to unauthorized individuals.

Threats countered:

- T.FARFRR
- T.IMPERSON

Security Objective for the TOE: O.FLAW

The TOE must not contain obvious flaws, whether intentional or unintentional, in its design, implementation, or operation.

Threats countered:

- T.FLAW
- T.BADDEV

Security Objective for the TOE: O.ADMIN

The TOE must limit TOE administrative functions to those verified as administrators by the TOE. The TOE must provide all the administrative functions necessary to support the management of TOE security and shall include functions to 1) tune the FAR/FRR; 2) maintain the enrolled images database; 3) manage auditing; 4) restore the Biometric Device to a secure state in the event of failure or interruption; 5) verify secure operation of the TOE.

Threats countered:

- T.FARFRR, T.AUDMOD,T.POWER
- T.BADUSER, T.BADOPER

Security Objective for the TOE: O.OPER

The TOE must limit operator functions to those verified as operators by the TOE and shall provide functions for routine maintenance and emergency startup/shutdown.

Threats countered:

- T.BADUSER
- T.BADADM
- T.POWER

Security Objective for the TOE: O.RECORD

The TOE must record necessary events to ensure that the information exists to support effective security management and must ensure that all TOE users can subsequently be held accountable for their security relevant actions.

Threats countered:

- T.AUDREV
- T.AUDMOD
- T.AUDFAIL

Security Objective for the TOE: O.NOMOD

The TOE must ensure that modification of security-relevant data, configuration items, audit parameters, and the audit trail is restricted to an authorized administrator.

Threats countered:

- T.CORRUPT
- T.AUDMOD

Security Objective for the IT Environment: O.PHYS

Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security.

Threats countered:

- T.ELECMAG
- T.RELAY1
- T.RELAY2

Security Objective for the non-IT Environment: O.INSTALL

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

Policies Supported:

- A.PHYSICAL
- A.RELAY
- A.SINGLE
- A.DEDICATED

Recent PP development work has resulted in the determination that assumptions are just that - “assumptions”, that is facts which are true and not needing support.

If O.INSTALL is needed it would be because these are listed as policies, not assumptions.

Security Objective for the non-IT Environment : O.BCKUP

A manual backup system exists and is properly installed. The procedures for manual operation are clearly outlined for the administrator. These procedures indicate how to implement the manual backup system in the event of a failure.

Policies supported:

- P.MANUAL

Security Objective for the non-IT Environment : O.NONNW

Those responsible for the TOE must ensure that the TOE is installed in a stand-alone manner and is not part of a network. In addition, the machine which supports the Biometric Device software must be configured as a dedicated machine.

Policies supported:

- A.DEDICATED
- A.SINGLE

Recent PP development work has resulted in the determination that assumptions are just that - "assumptions", that is facts which are true and not needing support.

If O.NONNW is needed it would be because these are listed as policies, not assumptions.

Security Objective for the non-IT Environment : O.TRAIN

Those responsible for the security of the organization must provide initial and ongoing training for all individuals, not just administrators. This training should include security awareness of vulnerabilities.

Policies supported:

- ~~A.NO_EVIL~~
- P.TRAIN

Workshop Schedule
Thursday

- 8am - 9am: Requirements Review
- 9:00am - noon: Requirements Selection Exercise
- noon - 1pm: Lunch
- 1pm - 4pm: Continue Exercise and Prepare Briefings